Volume 119
Issue 4 *Dickinson Law Review - Volume 119, 2014-2015*

3-1-2015

Computer Age Protesting: Why Hacktivism is a Viable Option for Modern Social Activists

Andrew T. Illig

Computer Age Protesting: Why Hacktivism is a Viable Option for Modern Social Activists

Andrew T. Illig*

ABSTRACT

Hacktivism, a term combining the words "hack" and "activism," is used to explain demonstrations that employ computers and the Internet to promote social or political goals. Individuals engaging in hacktivism, known as hacktivists, generally believe that information should be available to everyone without restriction. The hacktivism phenomenon predictably began in lock step with the development and proliferation of the Internet. Since its humble beginnings, hacktivism has become an increasingly common and effective means of communicating social justice messages.

Despite computers and other technology being used with increasing frequency, forms of free speech and expression are limited and defined according to old-fashioned ideologies. In addition, the availability of, and access to, traditional forums is declining. Current legislation prevents hacktivists from freely expressing their constructive messages in a public forum. Though creating an exemption or formulating a statutory amendment would be difficult, the rationale behind the First Amendment and other public policies support a calculated change to statutes like the Computer Fraud and Abuse Act ("CFAA").

This Comment attempts to propose a solution that would allow for certain hacktivist activities and provide solutions to the tension between free speech and Internet security. First, an amendment to the CFAA could require a hacktivist to notify the target after the fact and pay the minimal costs of network repair. Second, the CFAA could include an affirmative defense requiring a defendant to show that the actions taken were political or socially motivated under an objective reasonable person

* J.D. Candidate, The Dickinson School of Law of the Pennsylvania State University, 2015.

standard and that the damage or loss was minimal. A final option could be to implement an additional scienter requirement requiring that a defendant have a specific intent to cause irreparable harm or injury beyond a mere inconvenience.

Table of Contents

I. INTRODUCTION

Various forms of social activism have served as vehicles for the most radical social changes in history, including, for example, the Women's Suffrage Movement of the early 20th century and the Civil Rights Movement of the 1960s.[1] Today, in the age of the Internet, with

1. *See A Brief History of Women's Rights Movements*, SCHOLASTIC, http://bit.ly/1hnSkmk (last visited Nov. 5, 2013); Jack E. Davis, *Civil Rights Movement: An Overview*, SCHOLASTIC, http://bit.ly/1dQPl0L (last visited Nov. 5, 2013).

the newest generation increasingly connected to, and reliant on, technology, activism using computers seems to be a logical choice for socially conscious and technologically adept individuals.[2]

Under current law, however, particularly the Computer Fraud and Abuse Act ("CFAA"),[3] individuals have been limited in their use of the one tool that could reach the most people and have the greatest impact: the computer.[4] This is especially problematic given that available spaces for traditional protests have been declining, access to permitted venues is increasingly difficult, and the available venues are not where people congregate in large numbers.[5] Therefore, this Comment will argue that the CFAA should include an exemption to its criminal and civil provisions to allow for such activism provided that the individual shows a social purpose, takes responsibility, and makes appropriate reparations.

In order to understand why an exemption is desirable, Part II of this Comment will start by defining hacktivism and outlining some of its common forms. Part II will go on to detail the parameters of the CFAA and identify other potential legal authorities that might influence the regulation of hacktivism. Finally, Part III will analyze how the First Amendment, the CFAA and its legislative history, and public policy all counsel in favor of including a statutory exemption for certain hacktivist activities.

II. BACKGROUND

Though the term "hacktivism" was coined in 1996, the first serious cyber-attack with a documented political aim occurred in October 1989 when National Aeronautics and Space Administration ("NASA")[6] and the U.S. Department of Energy[7] computers were compromised, altering

2. *See Reduce Screen Time*, NAT'L HEART, LUNG, AND BLOOD INST., http://1.usa.gov/1a2EUtk (last visited Jan. 13, 2014).

3. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2006).

4. Computers can still be used for online activism and to promote social awareness through social media or other methods, but the types of hacktivism discussed in this Comment would likely be prohibited under the CFAA because it interferes with other people's computer systems. *See id.*; *infra* Parts II.B.1-6.

5. *See* John D. McCarthy & Clark McPhail, *Places of Protest: The Public Forum in Principle and Practice*, 11 MOBILIZATION: AN INT'L Q. 229 (2006).

6. NASA's vision is "[t]o reach for new heights and reveal the unknown so that what we do and learn will benefit all humankind." *See About NASA; What Does NASA Do?*, NASA, http://1.usa.gov/1EWbaM7 (last visited Feb. 10, 2015). Through space exploration, NASA seeks to answer basic questions about how Earth fits into the larger universe. *Id.* These questions include: "What's out there in space? How do we get there? What will we find? What can we learn there, or learn just by trying to get there, that will make life better here on Earth?" *Id.*

7. The U.S. Department of Energy seeks "to ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges through

log-in screens with an anti-nuclear message.[8] In a relatively short time, hacktivism has emerged as an effective avenue for social expression and discourse.[9]

A. What is Hacktivism?

Hacktivism is, predictably, created by combining the words "hack" and "activism."[10] Generally, hacktivism is defined as using computers to promote social or political ends or to effect social or political change.[11] The politics of civil disobedience are combined with the technological innovations and techniques of an increasingly computer-savvy public to create hacktivism.[12]

Using computer skills for personal monetary gain, often through identity theft, encompasses what many believe to be hacking.[13] Hacktivism, however, is different from its stigmatized cousin and is motivated not by individual gain, but by a larger social, political, or moral agenda.[14] A vast majority of the individuals engaged in hacktivism, also known as hacktivists, share a common trait: these individuals believe that information, and especially information on the Internet, should be free and accessible to all.[15]

---

transformative science and technology solutions." *Mission*, ENERGY.GOV, http://energy.gov/mission (last visited Feb. 10, 2015).

8. The message read, "WORMS AGAINST NUCLEAR KILLERS ... Your System Has Been Officially WANKed." *See* Ty McCormick, *Hacktivism: A Short History*, FOREIGN POLICY (Apr. 29, 2013), http://atfp.co/12TdO0W.

9. Alexandra Whitney Samuel, Hacktivism and the Future of Political Participation 2 (Sept. 2004) (unpublished Ph.D. dissertation, Harvard University), *available at* http://bit.ly/IMNPVc.

10. *Hacktivism*, MASHABLE, http://on.mash.to/GA1Ame (last visited Oct. 1, 2013).

11. Noa Bar-Yosef, *How Operation Payback and Hacktivism Are Rocking the 'Net*, SECURITY WEEK (Dec. 15, 2010), http://bit.ly/dJozxE.

12. Samuel, *supra* note 9, at 1-2.

13. Noah C.N. Hampson, Note, *Hacktivism: A New Breed of Protest in a Networked World*, 35 B.C. INT'L & COMP. L. REV. 511, 515 (2012).

14. *Id.* at 3.

15. *See* McCormick, *supra* note 8; Samuel, *supra* note 9, at 34. In an infamous move towards freedom of information and curbing government secrecy, WikiLeaks founder Julian Assange published information stolen by a United States Army veteran to his website. *See* Massimo Calabresi, *WikiLeaks' War on Secrecy: Truth's Consequences*, TIME (Dec. 2, 2010), http://ti.me/HLYOei. Assange published more than 250,000 diplomatic cables in what is the largest unauthorized contemporary disclosure of classified information in history. *Id.* Assange has been called the 'Robin Hood of Hacking' for his commitment to freedom of information. Eben Harrell, *WikiLeaks Found Julian Assange*, TIME (Jul. 26, 2010), http://ti.me/1fng1ql. The controversy has been immortalized in the recent DreamWorks film, "The Fifth Estate." *'The Fifth Estate,' Movie Review*, NY DAILY NEWS (Oct. 17, 2013), http://nydn.us/H6E0Og. This controversy is outside the scope of this Comment because of the stolen information

For some groups, faithfulness to freedom of information on the Internet is not simply a goal, but rather a membership requirement.[16] A hacking group known as "Hacktivismo" issued a "code of conduct" for online civil disobedience that represents this very ethos.[17] Hacktivismo proclaims their support for an uncensored Internet where civil rights are best served through "freedom of expression and opinion" and the "freedom to seek, receive, and impart information."[18] Because hacker culture places a premium on humor and artistry,[19] hacktivists take great pride in displaying their individual messages and anecdotes through technological superiority.[20]

Further, hacktivism can be distinguished from hacking and cyberterrorism because of its focus on and commitment to nonviolent forms of activism.[21] While cyberterrorists display a willingness to cause physical property damage and harm to human beings, hacktivists display a commitment to reaching meaningful social ends without jeopardizing human welfare.[22] Though this Comment focuses on hacktivist methods through the lens of social activism, cyberterrorists can potentially use these same methods for malignant purposes.[23]

Another distinction involves differentiating between hacktivism and traditional online activism, or cyberactivism.[24] Cyberactivism involves activities such as circulating online petitions, creating awareness sites, or providing online support to real world protests,[25] while hacktivism takes a more deviant approach by using currently illegal or legally ambiguous means to convey a message.[26] In the same way that traditional activists have the option to protest, boycott, or march, hacktivists have the option to choose between one of many forms of protest.[27]

---

involved, but the story serves to highlight the dedication among the hacker culture to the idea of freedom of information.

16. *The Hacktivismo Declaration*, HACKTIVISMO (July 4, 2001), http://bit.ly/JgZAS.
17. *Id.*
18. *Id.*
19. Samuel, *supra* note 9, at 7.
20. *Id.* at 8.
21. *Id.* at 3.
22. *Id.* at 3-4.
23. *Id.* at 3.
24. CYBERACTIVISM: ONLINE ACTIVISM IN THEORY AND PRACTICE 1 (Martha McCaughey & Michael D. Ayers eds., 2003).
25. *Id.*
26. Samuel, *supra* note 9, at 8
27. *Id.*

B. Common Forms of Hacktivism

The definition of hacktivism may be straightforward, but many forms exist. The differences among the common forms of hacktivism reflect hacktivist preferences and serve different functions.[28] Hacktivists choose their methods because they believe the surprise, novelty, and direct nature of the attacks are more effective than other forms of online activism or offline protests.[29]

1. Denial of Service Attacks

Denial of service attacks are one method hacktivists use to engage in political activism.[30] While not designed to gain access to the targeted system,[31] denial of service attacks, otherwise known as "DoS attacks," function by overwhelming a computer or network with a large volume of online activity, typically through the use of viruses or malware.[32] DoS attacks can be specific and target a single company or organization, or they can be general and target large portions of the Internet.[33] This form of hacktivism utilizes anonymous computer programs in a manner that simulates legitimate web page requests in order to occupy valuable computational power.[34]

One example of a denial of service attack occurred in August of 2013, when a four hour DoS attack shut down a portion of the Chinese Internet.[35] This attack overwhelmed a registry designed to convert the website names selected by Internet browsers into the numeric addresses that actually direct the online traffic.[36] Traffic levels were estimated to have dropped over 30 percent below the average as the attack crippled the registry and made Internet access slow and unreliable.[37] This attack on the Chinese Internet provides a clear illustration of the ability of DoS to substantially impair Internet programming.[38]

---

28. *Id.*
29. *Id.*
30. *Id.* at 10.
31. Samuel, *supra* note 9, at 10.
32. Paul Mozer, *Chinese Internet Hit by Attack Over Weekend*, WALL ST. J. CHINA REAL TIME (Aug. 26, 2013, 3:51 PM), http://on.wsj.com/142q9Ou. Malware, also known as "malicious software," is software designed to harm or disrupt the function of another computer. *See Malware*, TECHTERMS.COM, http://bit.ly/1M6QQtw (last visited Feb. 9, 2015).
33. Samuel, *supra* note 9, at 10.
34. G.F., *How Does a Denial-of-Service Attack Work?*, ECONOMIST (Mar. 31, 2015, 7:50 PM), http://econ.st/14BP0fO.
35. *Id.*
36. *Id.*
37. *Id.*
38. *See id.*

2. Virtual Sit-Ins

Virtual sit-ins, similar to DoS attacks, are a second form of hacktivism.[39] Unlike DoS attacks, which use viruses or malware to overload a target, virtual sit-ins instead consist of a large, organized group of people that will simultaneously, quickly, and repeatedly reload the targeted web page until the site becomes overloaded and slows down dramatically.[40] A large number of participants are more effective because greater numbers create a quicker and more sustained information overload.[41] Virtual sit-ins resemble a more traditional democratic or representative protest method because actual human beings, as opposed to the passive use of viruses or malware, are required to band together with a common goal in order to properly execute a virtual sit-in.[42]

For example, in April 2010, Ricardo Dominguez organized a student protest using the virtual sit-in method to encourage greater transparency from the president of the University of California.[43] Dominguez opted for an electronic approach instead of partaking in the contemporaneous traditional street protests, though both were organized in opposition of budget cuts and tuition increases.[44] The idea of the attack was to virtually occupy the president's office by jamming the Office of the President Portal[45] on the university system.[46] Although some criticized the attack as a harmful, prolonged, and unending DoS attack, supporters defended Dominguez's actions because the virtual sit-in was nothing more than an ordinary protest.[47] Despite the electronic platform, the protest was ordinary because the virtual sit-in was open, transparent, and used identifiable individuals rather than difficult to identify software.[48] Dominguez's protest illustrates the ways in which a virtual sit-in utilizes a large group of people to overwhelm a targeted web page.[49]

---

39. Samuel, *supra* note 9, at 12.
40. *Id.*
41. *Id.*
42. *Id.*
43. Steve Kolowich, *Virtual Sit-In*, INSIDE HIGHER ED (Apr. 9, 2010), http://bit.ly/bqEEAB.
44. *Id.*
45. According to the official website, the Office of the President Portal "is the systemwide headquarters of the University of California, managing its fiscal and business operations, and supporting the academic and research missions across its campuses, labs and medical centers." UNIVERSITY OF CALIFORNIA: OFFICE OF THE PRESIDENT, http://www.ucop.edu/ (last visited Jan. 15, 2014).
46. Kolowich, *supra* note 43.
47. *Id.*
48. *Id.*
49. *Id.*

3. Site Defacements

Site defacements, a third type of hacktivism, are similar to real world graffiti.[50] These are performed by accessing a web server and replacing or altering the content of a web site with some sort of political message.[51] Although traditional hackers use this technique,[52] hacktivists are distinguishable because of the messages' content, which is political and usually critical of the original web page's sponsor organization.[53]

An example of a site defacement occurred after September 11,[54] when a California international e-commerce firm's website, World Trade Services, was defaced with a message suggesting that the U.S. government organized the World Trade Center attacks in order to provide further justification for the Osama Bin Laden manhunt.[55] Although the hacktivists displayed an uncomfortable message for Americans to digest, such messages surrounding controversial current events often spark retaliatory action and competition among hacktivists to spread their individual messages.[56] This attack was retaliation against a separate group of hackers who disrupted Arabic sites and networks in the wake of the September 11 attacks.[57] Defacers commonly use their "attacks" as a means to exchange information and opinions in a public forum.[58] Site defacements, like the example above, illustrate the type of virtual graffiti used by hacktivists in order to convey their messages.[59]

50. Samuel, *supra* note 9, at 8.

51. *Id.*

52. Traditional hackers use site defacements to show individual technological prowess and communicate with other hackers. *Id.*

53. *Id.*

54. On September 11, 2001, four airliners hijacked by members of al-Qaeda, a terrorist organization then-based in Afghanistan, were used in an attack against the United States. *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 1-14 (2004). An airliner was deliberately crashed into both towers of the World Trade Center in New York City, a third was crashed into the Pentagon in Arlington County, VA, and the fourth was brought down by passengers in Shanksville, PA. *Id.* The death toll stands at just under 3,000. *Id.* The event, generally known as "9/11," was the catalyst for the Global War on Terror. *Id.*

55. *Pakistani Hackers Strike Back, Deface U.S. Site*, EXTREMETECH (Sept. 19, 2001), http://bit.ly/18U6bbM.

56. *Id.*

57. *Id.*

58. *Id.*

59. *See id.*; *see also* Samuel, *supra* note 9, at 8.

4. Site Redirects

Site redirects are a fourth form of hacktivism.[60] In order to execute a site redirect, a hacktivist accesses a web server and alters a web address, causing individuals to unwittingly find themselves on an undesired website, just as if someone switched around addresses in a phone book.[61] The final destination is often a site that is critical or in opposition of the desired site.[62] Normally the first sign of a site redirect is that traffic to the targeted website diminishes to an almost non-existent level.[63]

For example, a group called UGNazi[64] redirected UFC.com, coach.com, and coachfactory.com to ugnazi.com.[65] This redirect was a response to the martial arts company's and luxury accessory manufacturer's support of online piracy bills.[66] The redirect caused the desired effect of lowering traffic to the targeted sites and conveyed the desired message that hacktivists do not approve of the organizations' support of the online piracy bills.[67]

5. Site Parodies[68]

A fifth type of hacktivism comes in the form of site parodies.[69] A site parody occurs when a hacktivist creates a sham web page that mimics either the design or web address of the targeted site, or both, in

60. Samuel, *supra* note 9, at 10.

61. *Id.*

62. *Id.*

63. Tim Wilson, *Hacktivists Turn To DNS Hijacking*, INFORMATIONWEEK DARK READING (Jan. 26, 2012), http://ubm.io/1bAwJkA.

64. Short for Underground Nazi Hacker Group, UGNazi is a computer hacker group best known for DoS attacks and for opposing legislation such as the Cyber Intelligence Sharing and Protection Act and the Stop Online Piracy Act. *UGNazi*, KNOW YOUR MEME (last visited May 1, 2015) http://bit.ly/10Rxp0E.

65. Wilson, *supra* note 63. UGNazi redirected the traffic to a site with the address ugnazi.com, presumably to take credit for the attack and ensure that the target understood the reason for the demonstration. *See* Keith Dsouza, *Coach.com and Coachfactory.com Hacked to Protest Against SOPA by UGNazi Group*, TECHIE BUZZ (Jan. 24, 2012), http://bit.ly/1dGgP6o.

66. Wilson, *supra* note 63; Dsouza, *supra* note 65.

67. Wilson, *supra* note 63.

68. Because the parody sites may mimic or copy protected insignias or other intellectual property, site parodies may raise issues regarding misappropriation of intellectual property. *See generally* The Copyright Act of 1976, 17 U.S.C. §§ 101-107 (2006); The Trademark Act of 1946, 15 U.S.C. §§ 1051-58 (2006). These concerns, however, will not be addressed in this Comment because they are beyond the scope of the argument.

69. Samuel, *supra* note 9, at 13.

hopes that Internet users will find themselves on the sham web page,[70] rather than the intended one.[71] By using this method, a hacktivist creates an entirely separate site and attempts to capitalize on confusion or inattentive viewers, resulting in an individual selecting the parody site's link instead of the intended web page.[72] While site redirects rely on web server manipulation to channel a viewer away from the selected link and towards an opposition site,[73] site parodies do not manipulate web servers and instead result from the creation of entirely new web pages.[74] The site parody method requires no intrusion onto the targeted web page or organization's server, nor does this method compromise any information or security.[75]

For example, one parody site mimicked the National Security Agency's ("NSA")[76] website with a similar page layout and URL.[77] In light of the 2013 Snowden leaks and ensuing controversy,[78] this parody site sought to inform viewers about the privacy issues that accompany an increasing reliance on technology.[79] While most of the information on the site was accurate, the creator did not intend for people to mistake his site for the official NSA webpage, but instead just mimicked the site's address.[80] This parody site takes on an amusing tone as it asserts that the NSA[81] "embraces the openness about domestic intelligence gathering

70. The sham web page often, but not always, has a message in direct opposition to the desired site. *Id.*

71. *Id.*

72. *Id.*

73. Samuel, *supra* note 9, at 10.

74. *Id.* at 13.

75. *Id.*

76. The National Security Agency is the U.S. intelligence agency charged with producing signals intelligence. JAMES BAMFORD, BODY OF SECRETS: ANATOMY OF THE ULTRA-SECRET NATIONAL SECURITY AGENCY 146-47, 482 (2002). Estimated to be one of the largest of the 16 U.S. intelligence agencies in terms of personnel and budget, the agency is operated under the jurisdiction of the Department of Defense. *Id.*

77. Kashmir Hill, *The Definitive NSA Parody Site is Actually Informative*, FORBES (Aug. 29, 2013, 12:14 PM), http://onforb.es/14bn3aW. The legitimate webpage is nsa.gov, while the parody site URL, seeking to prey upon inattentive web surfers, is nsa.gov1.info. *Id.*

78. A former government contractor, Edward Snowden, leaked NSA documents related to surveillance within the continental United States and around the world. *See Timeline of Edward Snowden's Revelations*, AL JAZEERA AMERICA, http://alj.am/175wpow (last visited Nov. 5, 2013). Snowden fled the country and spent time in both Russia and Hong Kong. *Id.* The first leak related to the government requiring Verizon to turn over metadata on domestic phone calls to the Federal Bureau of Investigation. *Id.*

79. Hill, *supra* note 77.

80. *Id.*

81. This is in reference to the fake and parodied NSA, not the actual NSA. *See id.*

brought on by the Snowden leaks,"[82] but the true purpose of the parody site centers on providing information.[83] Site parodies do not interfere directly with the target site, unlike the next type of hacktivism, but instead try to capitalize on inattentive browsers by mimicking the target's web address or other identifying marks.[84]

6. Theft of Information

Finally, a sixth type of hacktivism is theft of information.[85] As the name suggests, theft of information involves accessing a private network and stealing private information.[86] Some hacktivists choose to sell or publish the stolen information, but generally the attacks are perpetrated to embarrass a company or highlight a lack of adequate security.[87] The public likely considers theft of information to be criminal and without any social value because tangible information changes hands without authorization.[88] Hacktivists, however, consider information theft to be a viable and available tool; the goal of the theft in this situation is generally to embarrass or shame an organization rather than to obtain or use the stolen information.[89] Because these forms of hacktivism may be used maliciously, Congress has acted to curtail these types of activities.

C. *The Computer Fraud and Abuse Act*

The CFAA criminalizes a broad range of activities.[90] The CFAA prohibits unauthorized access to computers that results in the perpetrator obtaining restricted data that could be used to injure the United States.[91] Further, unauthorized access that results in the perpetrator obtaining information from a financial institution, a U.S. department or agency, or a protected computer is prohibited.[92] Section 1030(a)(3) outlaws the intentional unauthorized access to any non-public computer of a U.S.

82. Hill, *supra* note 77.
83. *Id.*
84. Samuel, *supra* note 9, at 13
85. *Id.* at 11.
86. *Id.*
87. *Id.*
88. *Id.*
89. Samuel, *supra* note 9, at 11. Sometimes, however, information may be published on the Internet to enhance the effectiveness and embarrassment stemming from the attack. *Id.*
90. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2006). The CFAA has provisions that allow for civil claims; however, the statute's definitions apply to both classes of claims. *Id.* § 1030(g). The focus of this Comment will be on the criminal rather than civil penalties.
91. *Id.* § 1030(a)(1).
92. *Id.* § 1030(a)(2).

department or agency that is for government use.[93] The unauthorized access must affect that government use.[94] Other provisions outlaw knowingly accessing protected computers with intent to defraud;[95] knowingly, and with intent to defraud, trafficking computer access codes;[96] and intending to extort money by threatening computer damage through interstate communications.[97] Though civil remedies are possible, the legislative history suggests that Congress focused on amending federal criminal codes, such as the CFAA, because the laws before the CFAA's enactment were "insufficient to address the problem of computer crime."[98]

Unlike the other sections of the CFAA, § 1030(a)(5) does not require a perpetrator to obtain or traffic information[99] and therefore makes the section particularly applicable and relevant to potential hacktivists.[100] Section 1030(a)(5) prohibits actions in which an individual:

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally access a protected computer without authorization, and as a result of such conduct, causes damage and loss.[101]

A protected computer is defined as a computer "used or affecting interstate or foreign commerce or communication" and includes computers not located within the United States.[102] Access means to "obtain, acquire, or to gain admission to" a protected computer.[103] The terms "damage"[104] and "loss"[105] are both defined broadly, and courts

93. *Id.* § 1030(a)(3).
94. *Id.*
95. 18 U.S.C. § 1030(a)(4).
96. *Id.* § 1030(a)(6).
97. *Id.* § 1030(a)(7).
98. S. REP. NO. 99-432, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479.
99. 18 U.S.C. § 1030(a)(1)-(4), (6)-(7).
100. Id. § 1030(a)(5).
101. *Id.*
102. *Id.* § 1030(e)(2); *see also* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012).
103. *WEC Carolina Energy Solutions*, 687 F.3d at 204.
104. 18 U.S.C. § 1030(e)(8).
105. *Id.* § 1030(e)(11).

have required that a plaintiff show, at least in civil cases, either "damage" or "loss" but not both.[106]

The definition of damage includes "any impairment to the integrity or availability of data, a program, a system, or information."[107] At least one court provides the following, slightly different definition of damage: "transmission that weakens sound computer system – or, similarly, one that diminishes plaintiff's ability to use data or system."[108] The term "loss" includes "any reasonable cost to any victim . . . incurred because of interruption of service."[109] The valuation of "loss" is meant to include not only actual repairs, but also lost computer time, reliance costs of individuals who view altered information, and other incidental costs to the victim.[110] Further, in order to survive a summary judgment motion, the prosecutor must allege facts that connect the claimed "damage" or "loss" to the interruption of service.[111]

Penalties under the CFAA vary depending on the alleged act in question.[112] The available penalties included under the statute range from misdemeanor prison terms or minimal fines to maximum fines of $250,000 or twenty years in prison.[113] A life sentence is possible if the perpetrator has the specific intent to knowingly or recklessly cause the death of another individual.[114] Though important domestically, the CFAA must be analyzed in concert with other sources of law because the Internet is a multinational forum for communication.[115]

D. Other Authorities Potentially Binding on Hacktivists

Although the CFAA is an important statute, other authorities are potentially relevant and may address actions related to claims brought under the CFAA.[116] Because technology has the capability to access international locations with ease, cognizance of international law is also

106. Motorola, Inc. v. Lemko Corp., 609 F. Supp. 2d 760, 766-67 (N.D. Ill. 2009); *see also* Fiber Sys. Int'l, Inc. v. Roehrs, 470 F.3d 1150, 1157 (5th Cir. 2006); P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504, 511-12 (3d Cir. 2005); Theofel v. Farey-Jones, 359 F.3d 1066, 1078 n.3 (9th Cir. 2004).

107. *Id.* § 1030(e)(8).

108. Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 301 (6th Cir. 2011).

109. 18 U.S.C. at § 1030(e)(11)

110. S. REP. NO. 99-432, at 11-12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479

111. *See* CustomGuide v. CareerBuilder, LLC, 813 F. Supp. 2d 990, 998 (N.D. Ill. 2011)

112. 18 U.S.C. § 1030(c).

113. *Id.*

114. *Id.*

115. *See* Hampson, *supra* note 13, at 514.

116. *See generally id.*

necessary, though not specifically addressed in this Comment.[117] These various domestic and international statutes may all play a role in regulating an individual's actions depending on the applicable facts.

1. President Obama's February 2013 Executive Order[118]

President Obama's executive order titled "Improving Critical Infrastructure Cybersecurity" requires federal administrative agencies to assist private companies by creating a Cybersecurity Framework[119] designed to reduce the network security risks faced by private companies.[120] The purpose of the order is to minimize cyber threats through information sharing and the collaborative development and implementation of standards.[121] Sharing threats between government agencies and private companies will theoretically create a stronger infrastructure and increase the ability of the government and private sector companies to defend against cyber threats.[122] The executive order also encouraged Congress to pass further legislation designed to protect companies and individuals beyond the infrastructure created by the order.[123]

2. Electronic Communications Privacy Act[124]

Originally passed in 1986, the Electronic Communications Privacy Act ("ECPA") prohibits any person[125] from intercepting or disclosing the contents of any wire, oral, or electronic communication.[126] Because of President Obama's executive order[127] and criticisms that the ECPA is outdated because technology has changed drastically in the years since

117. *Id.*

118. Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

119. The framework "shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks" along with "voluntary consensus standards and industry best practices to the fullest extent possible" in order to effectively combat increased cyber threats. *Id.*

120. *Id.* at 11739-749; Grant Gross, *Obama Signs Cybersecurity Order*, CIO (Feb. 12, 2013), http://bit.ly/V9qmjY.

121. Exec. Order No. 13,636, 78 Fed. Reg. at 11739.

122. Gross, *supra* note 120.

123. Exec. Order No. 13,636, 78 Fed. Reg. at 11739

124. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-21, 2701-10 (2006).

125. Person is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

126. 18 U.S.C. § 2511.

127. Exec. Order No. 13,636, 78 Fed. Reg. at 11739

1986,[128] amendments to the ECPA are likely.[129] A proposed bill[130] included provisions prohibiting providers from disclosing stored communication content and revising the procedures by which the government, through a warrant, may obtain stored communication information from providers.[131] Though not enacted, this failed bill demonstrates the ongoing struggle for the legislature in responding to Internet related legal issues.

The American Civil Liberties Union[132] ("ACLU") is among the proponents for change.[133] The ACLU suggests that amendments should address location information transmitted from mobile devices, protect all personal electronic information, and require suppression of illegally obtained electronic information in the same way that non-electronic information is suppressed in court.[134] Further, the ACLU asks that legislators craft reasonable exceptions for emergency situations so long as individuals have proper notice and give informed consent.[135]

With the foregoing background in mind, this Comment will now examine how hacktivism can function in today's society in conjunction with criminal prohibitions like those laid out in the CFAA. For purposes of the following argument, it is important to remember that the particular method chosen by each hacktivist will differ depending on the circumstances. Further, though this Comment focuses on hacktivism in the context of the CFAA, other regulatory authorities, both domestic and international, are undoubtedly important and also play a significant role in influencing hacktivist behaviors.

III. ANALYSIS

For purposes of this analysis, and because the above methods could potentially be used by individuals without social or political motivations, hacktivism will only refer only to deviant and non-malicious actions prompted by social or political goals that do not cause extensive or

128. *Modernizing the Electronic Communications Privacy Act (ECPA)*, ACLU, http://bit.ly/qBeXVh (last visited Oct. 2, 2013).

129. *See* Electronic Communications and Privacy Amendments Act of 2013, H.R. 1847, 113th Cong. (1st Sess. 2013).

130. This bill was not enacted. *See* H.R. 1847.

131. *Id.*

132. The American Civil Liberties Union was founded to protect and preserve the individual rights guaranteed by the United States Constitution. *About the ACLU*, ACLU, http://bit.ly/1MakI8y (last visited Feb. 10, 2015).

133. *See* H.R. 1847.

134. *Id.*

135. *Id.*

lasting damage to the target.[136] Although those with malicious intent who cause extensive or lasting damage to a particular target through hacktivism should be prosecuted for the harm that they cause, hacktivism may be a legitimate activity for those individuals who wish to more innocently advocate for a particular social or political goal. With this limited definition in mind, potential exists for exemptions within current legislation that account for social activism through hacktivism. After analyzing the legal basis for an exemption, this Comment will recommend three possible solutions: a system of notification, a structured affirmative defense, and a heightened scienter requirement.

A. Hacktivism is a Viable Option for Modern Activists.

Multiple rationales support hacktivism as a legitimate option for technologically savvy activists. First, the guarantees of speech in the First Amendment[137] support the type of activism discussed in this Comment. Additionally, the legislative history of the CFAA and other public policy further support an exemption for certain hacktivist activities.

1. The First Amendment Supports Exclusion of Certain Hacktivist Activities From Coverage Under The CFAA.

The text of the First Amendment, in relevant part, reads as follows:

> Congress shall make no law . . . abridging the freedom of speech, or of the press; or of the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.[138]

The fundamental purpose of the First Amendment was to create a society in which information flowed freely and to preserve a marketplace of ideas where discussions and disputes were not inhibited by an oppressive government.[139] The U.S. Supreme Court has stated that "a

136. This distinction was made because this definition best encapsulates the goals of the First Amendment while at the same time protecting the government interest in computer and network security. The definition also helps to distinguish hacktivism from other forms of cyberactivism because it assumes some sort of legal ambiguity as opposed to innocent organizing or other efforts that do not directly interfere with target computers or networks. *See* Samuel, *supra* note 9, at 3. Further, this definition distinguishes hacktivism from cyberterrorism because the goal is social and political rather than malicious. *See* discussion *supra* Part II.A; *see also* Samuel, *supra* note 9, at 3

137. U.S. CONST. amend. I.

138. *Id.* The First Amendment also prohibits Congress from making laws that establish a national religion, *id.*, but that discussion is beyond the scope of this Comment.

139. *See* Simon & Schuster, Inc. v. Members of the New York State Crime Victims Bd., 112 S. Ct. 501, 508 (1991); Garrison v. Louisiana, 379 U.S. 64, 74-75 (1964).

function of free speech under our system of government is to invite dispute. Free speech may indeed best serve its high condition when it induces a condition of unrest, creates dissatisfaction with conditions as they are, or even stirs people to anger."[140] The freedoms of speech and press are not without limitations,[141] but the presumption is always in favor of protecting, rather than regulating, the content of speech.[142]

Courts have recognized that certain types of speech possess the potential for great harm,[143] but they have also upheld protections of speech with only questionable worth.[144] Originally, the First Amendment applied only to the federal government, but with the adoption of the Fourteenth Amendment,[145] the freedoms of speech and press were incorporated and became enforceable against state governments.[146] Because the presumption favors permitting speech,[147] and the First Amendment was written with the fundamental purpose of promoting a marketplace of ideas,[148] hacktivist methods should be protected by these First Amendment guarantees.

2. The Legislative History of the CFAA Supports a Statutory Exemption Allowing for Certain Hacktivist Activities.

A Senate Report explains that Congress's main concern in enacting the CFAA was to remedy the inadequacy of the then-current federal Criminal Code in dealing with the contemporaneous "technological explosion" and related negative behavior.[149] Protecting computers and sensitive electronic information is a laudable justification for a federal criminal statute; however, this justification must take other concerns into account, namely the rights protected by the First Amendment.[150] The Senate Report also acknowledged that the most effective means of defending against computer crime is not through a federal criminal statute, but through self-protection.[151]

---

140. *Id.*

141. *See, e.g.*, Brandenburg v. Ohio, 395 U.S. 444, 449 (1969); New York Times Co. v. Sullivan, 376 U.S. 254, 265 (1964).

142. Thomas v. Board of Educ., 607 F.2d 1043, 1047 (2d Cir. 1979).

143. *See, e.g.*, Gertz v. Robert Welch, Inc., 418 U.S. 323, 340 (1974); Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942).

144. *See Thomas*, 607 F.2d at 1047.

145. U.S. CONST. amend. XIV.

146. *See* Edwards v. South Carolina, 372 U.S. 229, 235 (1963).

147. *Thomas*, 607 F.2d at 1047.

148. *See* Simon & Schuster, Inc. v. Members of the New York State Crime Victims Bd., 112 S. Ct. 501, 508 (1991); Garrison v. Louisiana, 379 U.S. 64, 74-75 (1964).

149. S. REP. NO. 99-432, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479.

150. *See* U.S. CONST. amend. I; *see also* discussion *supra* Part III.A.1.

151. S. REP. NO. 99-432, at 3.

Congress specifically refused to "enact as sweeping a federal statute as possible so that no computer crime is potentially uncovered," but instead wished to limit the statute to those crimes in which a "compelling Federal interest" existed.[152] This "compelling Federal interest" presumably refers to protection of restricted or sensitive data, prevention of fraud, or criminalization of extortion through the use of unauthorized computer access.[153] Thus, absent from the intended realm of the "compelling Federal interest[s]" are the minimally invasive actions taken by hacktivists that cause limited interruptions.[154]

Congress added "damages or destroys" to § 1030(a)(5) because drafters wanted to ensure that the CFAA covered actions beyond "mere alteration of information," such as data deletion.[155] This addition supports the inference that the CFAA was designed to protect against specifically malignant actions rather than actions whose primary purpose is to affect social change.[156] The concern highlighted by this addition is not implicated by hacktivism because, though targeted individuals or companies experience some inconveniences, the goal of hacktivism is not to alter or erase information, but to draw attention to perceived injustices.[157]

Hacktivists, in the narrow sense addressed in this Comment, are not focused on destroying property or stealing information, but instead seek to inform the public or to protest organizations through the various demonstration methods detailed above.[158] However, under the broad definitions of "damage" and "loss" in the CFAA, even the most harmless cyber protests could be considered criminal[159] despite congressional intent to reign in malignant behavior, rather than socially conscious behavior.[160]

Hacktivism undoubtedly inconveniences targeted sites, but most methods do not permanently impair the target's web site. For example, a site redirect technically impairs the availability of data[161] because the hacktivist channels traffic from the desired site to a different site.[162]

152. *Id.* at 4. The "compelling Federal interest" referenced was computers used or affecting interstate commerce. *Id.*
153. *Id.*
154. *See id.*
155. *See id.* at 5.
156. S. REP. NO. 99-432, at 5.
157. *See* discussion *supra* Part II.A
158. *See supra* Part II.A, notes 30-89.
159. *See* Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a) (2006).
160. *See* S. REP. NO. 99-432, at 5.
161. *See* 18 U.S.C. § 1030(e)(8).
162. *See supra* Part II.B.4

Similarly, a DoS attack slows connection to a desired site.[163] However, in both examples, the security and content of the site remains unchanged.

Further, when examining the legislative history through the lens of the rule of lenity, a statutory exemption seems to be required.[164] The rule of lenity states that "the judicial doctrine holding that a court, in construing an ambiguous criminal statute . . . should resolve the ambiguity in favor of the more lenient punishment."[165] The rule of lenity counsels in favor of the defendant and a narrow statutory construction when the statute's express terms are ambiguous.[166] Despite the broad definitions provided by the CFAA, the CFAA's legislative history and the rule of lenity seem to allow for an exemption for hacktivism so long as hacktivists remain within the bounds of their social and political purpose and do not attack computer systems with criminal intentions.[167]

Because the statute is written in such a broad manner, even demonstrations like virtual sit-ins would be covered because they impair the integrity of a computer system.[168] In a virtual sit-in, however, no network security is compromised, no information is stolen, and no information or content is altered.[169] The breadth of the CFAA creates ambiguity and casts doubt on the legality of generally harmless activities. The rule of lenity counsels that this ambiguity should be resolved in favor of a defendant.[170] To avoid this confusion in court, the legislature should clarify that hacktivists are a class not meant to be covered under the CFAA. In concert with free speech concerns and the original purpose of the statute, a narrower definition of damage and loss is plausible, especially when no permanent damage is done by the hacktivist methods discussed above.[171]

3. Public Policy Supports Statutory Exclusion.

As the previous discussion of the First Amendment illustrates, the purpose in ratifying the First Amendment was to encourage public discourse and the exchange of ideas regardless of the palatability of the

163. *See supra* Parts II.B.1, II.B.4

164. BLACK'S LAW DICTIONARY 1449 (9th ed. 2009); *see generally* S. REP. NO. 99-432.

165. BLACK'S LAW DICTIONARY 1449 (9th ed. 2009).

166. *See id.*; *see also* United States v. Turkette, 452 U.S. 576, 587 n.10 (1981) (refusing to apply the rule of lenity because the statute, by its express terms, was unambiguous).

167. *See generally* S. REP. NO. 99-432; BLACK'S LAW DICTIONARY 1449 (9th ed. 2009).

168. *See* 18 U.S.C. § 1030 (e)(8); discussion *supra* Part II.B.2.

169. *See* discussion *supra* Part II.B.2

170. BLACK'S LAW DICTIONARY 1449 (9th ed. 2009).

171. *See supra* Parts II.B.1–6

belief.[172] In order to promote a successful democratic society and avoid oppressive institutions, a free market of ideas is necessary so that all voices may be heard and appreciated.[173] Hacktivists embrace this free market ideology and, through the computer, can effectively advance their positions and reach large audiences. This free market ideology will challenge traditional modes of thinking and help to promote critical thinking about important issues rather than blindly following or viewing recurring issues through the same old lenses. New perspectives should be welcomed, not discouraged.

B. Calculated Changes to the CFAA Would Allow for Protection of Computers and Free Speech Rights.

The Internet is shaped by various factors. Lawrence Lessig examines four different modalities of influence in cyberspace as he acknowledges the law's limitations with respect to Internet regulation.[174] Law, social norms, economic markets, and the physical architecture of the Internet all play a role in determining the development of Internet regulation.[175] Thus, any Internet statute or regulation will, according to Lessig, be a result of the interplay between one or more of these modalities depending on the specific issue.[176]

With Lessig in mind and before discussing possible amendments or exemptions to the statute, it should be noted that any change introduced to the statute should be written with caution. An improperly worded change to the statute may allow for criminally minded individuals to feign social motives in order to avoid liability. Because the Internet has become a part of everyday life, the law should accommodate certain computer related activities despite the tension that such accommodation may cause. With those limitations in mind, however, the below

172. *See* Simon & Schuster, Inc. v. Members of the New York State Crime Victims Bd., 112 S. Ct. 501, 508 (1991); Garrison v. Louisiana, 379 U.S. 64, 74-75 (1964).

173. *See* Terminiello v. Chicago, 69 S. Ct. 894, 896 (1949); *see also* discussion *supra* Part III.A.1.

174. *See* Lawrence Lessig, *Commentary: The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 507 (1999).

175. *Id.*

176. *See id.* The CAN-SPAM Act serves as an illustration of a legal response to an Internet issue, *see* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. § 7704 (2006) (regulating interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail), while various privacy policies serve as a market response to consumer concern over the privacy of their personal information. *See, e.g.*, *Privacy & Terms*, GOOGLE, http://bit.ly/1D3Gvbz (last visited, Jan. 27, 2015); *Data Use Policy*, FACEBOOK, https://www.facebook.com/policy.php (last visited, Jan. 27, 2015).

suggested statutory exemptions[177] should be strongly considered because of the overwhelming free speech issues and societal movement towards the increasing use of technology. Like many other times in history, the law should be cognizant of, and adapt as best as possible to, societal momentum.[178]

Admittedly, a few of the hacktivist methods outlined above, such as site defacements, site redirects, and theft of information, are clearly illegal under the CFAA.[179] However, other methods of hacktivism are more legally ambiguous in that they do not involve direct access to another's system, and therefore, the statutory change would be easier and need only be minimal in order to clarify to enforcing agencies that these methods are acceptable.[180] Further, these ambiguous methods, such as virtual sit-ins and site parodies, already seem more acceptable because hacktivists use traceable identifiers[181] as opposed to more frightening anonymous attacks. Whether the means are currently illegal or only of ambiguous legality, a proper statutory change would resolve these issues.

1. Notification

The effectiveness of a hacktivist attack lies in its spontaneity and directness;[182] therefore, a potential statutory amendment could include a notification exemption to the statutory penalties. In order to avoid penalties, this notification proposal would require the perpetrator to notify the target or take credit for the attack within a certain statutorily defined time period after the demonstration occurs. Further, any inconvenience suffered by the target could be charged to the perpetrator just as if an individual were paying a permit fee to organize an in-person

177. *See infra* Parts III.B.1—3.

178. *See generally* Loving v. Virginia, 388 U.S. 1 (1967) (holding that Virginia's ban on interracial marriage was unconstitutional); Brown v. Bd. of Educ., 347 U.S. 483 (1954) (holding that *Plessy v. Ferguson*'s racially discriminatory doctrine of "separate but equal" was unconstitutional, reasoning instead that "separate educational facilities are inherently unequal").

179. These three methods involve illegal access to, and interference with, computer networks, which falls directly within the CFAA's definition of "damage." *See* discussion *supra* Parts II.B.3–4, II.B.6, II.C.

180. Virtual sit-ins, *supra* Part II.B.2, and site parodies, *supra* Part II.B.5, are legally ambiguous because they do not directly interfere with or affect computer integrity under the CFAA. However, these methods funnel web traffic away from a target site and therefore indirectly interfere with the target site rather than directly attempt to disrupt the functionality of the target site.

181. Generally, real names or at least easily traceable aliases are used. S*ee* Samuel, *supra* note 9, at 37, 49

182. *See id.* at 3.

demonstration.[183] If a hacktivist stays within the narrow definition advocated in this Comment, minimal time will be required by the target to return a web page or server to its pre-demonstration state.

This approach would maintain the spontaneity of the attack and hopefully ensure maximum effectiveness. On the other hand, the spontaneity also hinders the target because the target is unable to prepare for, or prevent, the event. The target's response, therefore, becomes a reactionary system fix instead of a proactive solidification of a system's security. Damage occurs because the response is reactionary and involuntary, but the spontaneity allows the protestor actions to retain their maximum effectiveness. However, because the damage would be minimal and the permit–type fee would be designed to compensate the target, any loss due to a reactionary response would be appropriately taken into account. Before drafting such a notification amendment, legislators would have to determine whether the permit-type fee would adequately compensate a target's reactionary response to a spontaneous demonstration.

2. Affirmative Defense

Black's Law Dictionary defines an affirmative defense as "a defendant's assertion of facts and arguments that, if true, will defeat the plaintiff's or prosecution's claim, even if all the allegations in the complaint are true."[184] In other words, a defendant admits that he or she committed the acts in question, but the affirmative defense provides a justification for the acts.[185] Examples of affirmative defenses include duress,[186] insanity,[187] and self-defense.[188]

183. *See, e.g.*, *Parade Permits*, PITTSBURGH BUREAU OF BUILDING INSPECTION, http://bit.ly/1iTwIfd (last visited Feb. 10, 2014) (explaining that in the city of Pittsburgh, PA, applicants must produce identification, provide an overview of their parade or procession, provide names of those in charge, and pay a fee based on the event in question). Pittsburgh, PA requires a $25.00 fee for any application and an additional fee depending on the permit requested. *See Permit Fees*, PITTSBURGH BUREAU OF BUILDING INSPECTION, http://bit.ly/1dLM0xh (last visited Feb. 10, 2014). The U.S. Supreme Court upheld the constitutionality of state statutes requiring parade permits for demonstrations on public grounds. Cox v. New Hampshire, 312 U.S. 569, 577-78 (1941).

184. BLACK'S LAW DICTIONARY 1837 (9th ed. 2009).

185. *See id.*

186. Duress is an affirmative defense asserting that the actor performed the conduct in question but only because he or she was coerced to do so by the use of, or threat to use, unlawful force against the actor. MODEL PENAL CODE § 2.09(1) (2001).

187. Insanity is an affirmative defense in which a defendant argues that a mental disorder caused the individual to commit the crime in question. BLACK'S LAW DICTIONARY 1912 (9th ed. 2009).

An affirmative defense amendment to the CFAA would allow for the burden to be placed on a defendant, once the prosecutor proves all elements of the crime, to show that the damage or loss was minimal, if any. Further, this affirmative defense could have a second element requiring a defendant to show that the actions were socially motivated under an objective reasonable person standard rather than subjectively motivated by individual pecuniary gain. Presumably, if the action was taken for purposes other than social protest, the primary motivation would be destruction of the target web site or servers. A further presumption is that the political or social motivation will keep damage to a minimum, as opposed to an individual motivated by selfish or pecuniary reasons who likely has much less concern for such consequences.

These presumptions support a favorable inference for the defendant hacktivist. Once a defendant shows minimal damage, the mere fact that minimal damage occurred would indicate that social or political reasons inspired the actions, thus satisfying the second element of the affirmative defense. Of course, situations could arise where minimal damage will not always clearly point to social or political motivation. A failed attack for pecuniary gain could result in minimal damage just like a socially or politically motivated demonstration. Introduction of evidence by the prosecution that the defendant stole or acquired protected information, evidence that lasting damage occurred, or evidence indicating that the defendant's motivations were personal could be used to rebut a defendant's affirmative defense. This suggested affirmative defense would maintain the integrity of the criminal code by allowing the prosecution of suspected criminals. However, this maintenance of integrity would be balanced against the societal concerns of free speech and historical right to political activism.

3. Heightened Scienter Requirement

A final possible amendment to the CFAA could include a specific intent provision requiring a prosecutor to prove that the defendant had a specific intent to cause significant or irreparable damage to the target beyond a mere inconvenience. This enhanced mens rea requirement would require knowledge of specific facts that give rise to criminal liability. Thus, the defendant would have to possess specific knowledge

188. Self-defense occurs when an individual uses force to protect oneself, one's family, or one's property from a real or threatened attack. BLACK'S LAW DICTIONARY 1651 (9th ed. 2009).

that his or her actions were likely to cause significant or irreparable damage to the target.

For example, in *Staples v. United States*,[189] the prosecution was required to prove that the defendant knew the weapon he possessed had a certain characteristic[190] that brought the weapon within the statutory definition of prohibited firearms.[191] Because the defendant did not know he possessed a fully automatic weapon, and no evidence was introduced to the contrary, his conviction was overturned.[192] The *Staples* Court utilized the Signaling Theory, which uses innocence as a term of art, and postulates that certain activities do not signal to a defendant that the conduct undertaken is per se illegal.[193] In *Staples*, the Court stated that owning a gun is normal, pervasive behavior and does not put an individual on notice that one should question or research the legality of such ownership.[194]

Like the defendant in *Staples*, a hacktivist could argue that social activism is a normal, pervasive behavior that does not require specific knowledge about the act in question.[195] Despite the negative connotations associated with traditional hacking, a hacktivist could argue that online demonstrations are "innocent" as the term is used in *Staples*, because the intent is not destructive and the consequences, if any, are minimal and short-lived.[196]

In light of the Signaling Theory, many hacktivists likely choose targets without ever considering the illegality of their actions. According to the hacktivist belief system, information should be readily accessible to all.[197] If this belief system is combined with the First Amendment and the free market rationale that inspired its enactment,[198] the illegality of redirecting a site's web traffic[199] or organizing a virtual sit-in to protest a university's administration[200] may never cross a hacktivist's mind. Without a specific malicious intent or knowledge that certain actions are illegal rather than democratic, an individual cannot be said to be acting with requisite intent that indicates criminal culpability.

189. Staples v. United States, 511 U.S. 600 (1994).
190. Specifically, that the defendant knew the weapon was fully automatic. *Id.* at 600, 604.
191. *Id.* at 604.
192. *Id.* at 619.
193. *Id.* at 615, fn. 11.
194. *See Staples*, 511 U.S. at 615-16.
195. *Id.*
196. *Id.*
197. *See supra* Part II.A.
198. *See supra* Part III.A.1.
199. *See* discussion *supra* Part II.B.4
200. *See* discussion *supra* Part II.B.2

IV. CONCLUSION

Cybersecurity is a serious and legitimate concern.[201] Despite this concern, it seems odd that a country with a rich history of free expression would pass such a broad statute like the CFAA, which is written in a way that ignores legitimate means of demonstrating and participating in the democratic process. Congress has multiple options that would help alleviate this conflict, including a notification provision, an affirmative defense provision, or a heightened scienter requirement. In an age in which computer use is increasing[202] and available forums for traditional protest are shrinking,[203] criminalizing socially conscious hacktivist activities seems illogical.

201. *See* Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 19, 2013); *see also* Brian B. Kelly, Note, *Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*, 92 B.U. L. Rev. 1663, 1674-75 (2012).

202. *See* NAT'L HEART, LUNG, AND BLOOD INST., *supra* note 2.

203. *See* McCarthy & McPhail, *supra* note 5, at 237.

***